CLAIMS

What is claimed is:

1. A method for providing shared secret keys for communicating through a secure channel between members of a dynamically changing multicast group connected over an insecure network, the method comprising the computer-implemented steps of:

computing a first shared secret key for establishing a first multicast group that includes a set of one or more first members;

generating a first multicast group exchange key based on the first shared secret key;

receiving a first user exchange key from a first user requesting entry into the first multicast group;

computing a second secret key based on the first user exchange key and the first shared secret key;

sending the first multicast group exchange key to the first user, wherein the first multicast group exchange key allows the first user to generate the second shared secret key; and

establishing a second multicast group whose members include the first user and the set of one or more first members of the first multicast group, wherein the second shared secret key provides a first secure channel for communicating between members of the second multicast group over the insecure network.

2. The method as recited in Claim 1, wherein the step of computing a first shared secret key includes the steps of:

selecting a private non-zero random integer "x";

selecting a public non-zero integer "g";

selecting a public prime integer "n"; and

computing the first shared secret key "k" according to the relation

$k = (g^x \bmod (n))$.

3. The method as recited in Claim 2, wherein the step of generating a first multicast group exchange key includes the step computing the first multicast group exchange key K' according to the relation

$$K' = (g^k \bmod (n)).$$

4. The method as recited in Claim 2, wherein

the step of receiving a first user exchange key includes the step of receiving a first user exchange key value Y' computed according to the relation

$$Y' = (g^y \bmod (n)),$$

wherein "y" is a private non-zero random integer selected by the first user; and

the step of computing a second secret key includes the step computing the second secret key "k1" according to the relation

$$k1 = (Y'^k \bmod (n)).$$

5. The method as recited in Claim 2, wherein the step of sending the first multicast group exchange key to the first user further comprises the first user computing the second secret key "k1" according to the relation

$$k1 = (K'^y \bmod (n)).$$

6. The method as recited in Claim 1, wherein:

the step of receiving a first user exchange key from a first user comprises the step of verifying that the first user should be allowed entry into the first multicast group; and

providing the first user with the first multicast exchange key only after the first user is verified for entry into the first multicast group.

7. The method as recited in Claim 1, further comprising the steps of:

generating a second multicast group exchange key based on the second shared secret key;

receiving a second user exchange key from a second user requesting entry into the second multicast group;

computing a third secret key based on the second user exchange key and the second shared secret key;

sending the second multicast group exchange key to the second user, wherein the second multicast group exchange key allows the second user to generate the third shared secret key; and

establishing a third multicast group whose members include the second user and the members of the second multicast group, wherein the third shared secret key provides a second secure channel for communicating between members of the third multicast group over the insecure network.

8. The method as recited in Claim 2, further comprising the steps of:

determining that a first departing member has left the second multicast group;

selecting a private multicast group non-zero random integer;

generating a second multicast group exchange key based on the private multicast group non-zero random integer, the public non-zero integer "g" and the public prime integer "n";

broadcasting the second multicast group exchange key to each remaining member of the second multicast group;

in response to receiving the second multicast group exchange key, each remaining member computing a third secret key based on the second multicast group exchange key and the second shared secret key; and

establishing a third multicast group whose members include only remaining members of the second multicast group, wherein the third shared secret key provides a second secure channel for communicating between members of the third multicast group over the insecure network.

9. The method as recited in Claim 1, wherein the step of establishing a second multicast group requires a total of approximately N+1 messages for providing the first secure channel for communicating between members of the second multicast group over the insecure network.

10. A computer-readable medium carrying one or more sequences of one or more instructions for communicating through a secure channel between members of a dynamically changing multicast group connected over an insecure network, and which instructions, when executed by one or more processors, cause the one or more processors to perform the steps of:

computing a first shared secret key for establishing a first multicast group that includes a set of one or more first members;

generating a first multicast group exchange key based on the first shared secret key;

receiving a first user exchange key from a first user requesting entry into the first multicast group;

computing a second secret key based on the first user exchange key and the first shared secret key;

sending the first multicast group exchange key to the first user, wherein the first multicast group exchange key allows the first user to generate the second shared secret key; and

establishing a second multicast group whose members include the first user and the set of one or more first members of the first multicast group, wherein the second shared secret key provides a first secure channel for communicating between members of the second multicast group over the insecure network.

11. The computer-readable medium as recited in Claim 10, wherein the step of computing a first shared secret key includes the steps of:

selecting a private non-zero random integer "x";

selecting a public non-zero integer "g";

selecting a public prime integer "n"; and

computing the first shared secret key "k" according to the relation

$k = (g^x \bmod (n))$.

12. The computer-readable medium as recited in Claim 11, wherein the step of generating a first multicast group exchange key includes the step computing the first multicast group exchange key K' according to the relation

$$K' = (g^k \bmod (n)).$$

13. The computer-readable medium as recited in Claim 11, wherein

the step of receiving a first user exchange key includes the step of receiving a first user exchange key value Y' computed according to the relation

$$Y' = (g^y \bmod (n)),$$

wherein "y" is a private non-zero random integer selected by the first user; and

the step of computing a second secret key includes the step computing the second secret key "k1" according to the relation

$$k1 = (Y'^k \bmod (n)).$$

14. The computer-readable medium as recited in Claim 11, wherein the step of sending the first multicast group exchange key to the first user further comprises the first user computing the second secret key "k1" according to the relation

$$k1 = (K'^y \bmod (n)).$$

15. The computer-readable medium as recited in Claim 10, wherein:

the step of receiving a first user exchange key from a first user comprises the step of verifying that the first user should be allowed entry into the first multicast group; and

providing the first user with the first multicast exchange key only after the first user is verified for entry into the first multicast group.

16. The computer-readable medium as recited in Claim 10, further comprising instructions for performing the steps of:

generating a second multicast group exchange key based on the second shared secret key;

receiving a second user exchange key from a second user requesting entry into the second multicast group;

computing a third secret key based on the second user exchange key and the second shared secret key;

sending the second multicast group exchange key to the second user, wherein the second multicast group exchange key allows the second user to generate the third shared secret key; and

establishing a third multicast group whose members include the second user and the members of the second multicast group, wherein the third shared secret key provides a second secure channel for communicating between members of the third multicast group over the insecure network.

17. The computer-readable medium as recited in Claim 11, further comprising instructions for performing the steps of:

determining that a first departing member has left the second multicast group;

selecting a private multicast group non-zero random integer;

generating a second multicast group exchange key based on the private multicast group non-zero random integer, the public non-zero integer "g" and the public prime integer "n";

broadcasting the second multicast group exchange key to each remaining member of the second multicast group;

in response to receiving the second multicast group exchange key, each remaining member computing a third secret key based on the second multicast group exchange key and the second shared secret key; and

establishing a third multicast group whose members include only remaining members of the second multicast group, wherein the third shared secret key provides a second secure channel for communicating between members of the third multicast group over the insecure network.

18. The computer-readable medium as recited in Claim 10, wherein the step of establishing a second multicast group requires a total of approximately N+1 messages for providing the first secure channel for communicating between members of the second multicast group over the insecure network.

19. A network device configured for communicating through a secure channel between members of a dynamically changing multicast group connected over an insecure network, comprising:

a network interface;

a processor coupled to the network interface and receiving information from the network interface;

a computer-readable medium accessible by the processor and comprising one or more sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

computing a first shared secret key for establishing a first multicast group that includes a set of one or more first members;

generating a first multicast group exchange key based on the first shared secret key;

receiving a first user exchange key from a first user requesting entry into the first multicast group;

computing a second secret key based on the first user exchange key and the first shared secret key;

sending the first multicast group exchange key to the first user, wherein the first multicast group exchange key allows the first user to generate the second shared secret key; and

establishing a second multicast group whose members include the first user and the set of one or more first members of the first multicast group, wherein the second shared secret key provides a first secure channel for communicating between members of the second multicast group over the insecure network.

20. The network device as recited in Claim 19, wherein the step of computing a first shared secret key includes the steps of:

selecting a private non-zero random integer "x";

selecting a public non-zero integer "g";

selecting a public prime integer "n"; and

computing the first shared secret key "k" according to the relation

$k = (g^x \bmod (n))$.

21. The network device as recited in Claim 20, wherein the step of generating a first multicast group exchange key includes the step computing the first multicast group exchange key K' according to the relation

$K' = (g^k \bmod (n))$.

22. The network device as recited in Claim 20, wherein

the step of receiving a first user exchange key includes the step of receiving a first user exchange key value Y' computed according to the relation

$Y' = (g^y \bmod (n))$,

wherein "y" is a private non-zero random integer selected by the first user; and

the step of computing a second secret key includes the step computing the second secret key "k1" according to the relation

$k1 = (Y'^k \bmod (n))$.

23. The network device as recited in Claim 20, wherein the step of sending the first multicast group exchange key to the first user further comprises the first user computing the second secret key "k1" according to the relation

$k1 = (K'^y \bmod (n))$.

24. The network device as recited in Claim 19, wherein:

the step of receiving a first user exchange key from a first user comprises the step of verifying that the first user should be allowed entry into the first multicast group; and

providing the first user with the first multicast exchange key only after the first user is verified for entry into the first multicast group.

25. The network device as recited in Claim 19, further comprising instructions for performing the steps of:

generating a second multicast group exchange key based on the second shared secret key;

receiving a second user exchange key from a second user requesting entry into the second multicast group;

computing a third secret key based on the second user exchange key and the second shared secret key;

sending the second multicast group exchange key to the second user, wherein the second multicast group exchange key allows the second user to generate the third shared secret key; and

establishing a third multicast group whose members include the second user and the members of the second multicast group, wherein the third shared secret key provides a second secure channel for communicating between members of the third multicast group over the insecure network.

26. The network device as recited in Claim 20, further comprising instructions for performing the steps of:

determining that a first departing member has left the second multicast group;

selecting a private multicast group non-zero random integer;

generating a second multicast group exchange key based on the private multicast group non-zero random integer, the public non-zero integer "g" and the public prime integer "n";

broadcasting the second multicast group exchange key to each remaining member of the second multicast group;

in response to receiving the second multicast group exchange key, each remaining member computing a third secret key based on the second multicast group exchange key and the second shared secret key; and

establishing a third multicast group whose members include only remaining members of the second multicast group, wherein the third shared secret key provides a

second secure channel for communicating between members of the third multicast group over the insecure network.

27. The network device as recited in Claim 19, wherein the step of establishing a second multicast group requires a total of approximately N+1 messages for providing the first secure channel for communicating between members of the second multicast group over the insecure network.

28. A network device configured for communicating through a secure channel between members of a dynamically changing multicast group connected over an insecure network, comprising:

means for computing a first shared secret key for establishing a first multicast group that includes a set of one or more first members;

means for generating a first multicast group exchange key based on the first shared secret key;

means for receiving a first user exchange key from a first user requesting entry into the first multicast group;

means for computing a second secret key based on the first user exchange key and the first shared secret key;

means for sending the first multicast group exchange key to the first user, wherein the first multicast group exchange key allows the first user to generate the second shared secret key; and

means for establishing a second multicast group whose members include the first user and the set of one or more first members of the first multicast group, wherein the second shared secret key provides a first secure channel for communicating between members of the second multicast group over the insecure network.

29. A method for generating a shared secret key for use by a first member, a second member, and a third member who joins the first member and the second member for secure communication as a multicast group over an insecure network, the method comprising the computer-implemented steps of:

generating a first multicast group exchange key K' based on a first shared secret key "k" that is used by a first multicast group that includes the first member and the second member, wherein $k = (g^x \bmod (n))$, "x" is a private non-zero random integer, "g" is a public non-zero integer, and "n" is a pre-determined public prime integer, and wherein $K' = (g^k \bmod (n))$;

receiving a first user exchange key from the third member as part of a request by the third member to enter the first multicast group;

sending the first multicast group exchange key to the first member, wherein the first multicast group exchange key allows the first member to generate a second secret key based on the first user exchange key and the first shared secret key; and

establishing secure communication in a second multicast group whose members include the first member, the second member and the third member, and based on the second shared secret key.

30. The method as recited in Claim 29, wherein

the step of receiving a first user exchange key includes the step of receiving a first user exchange key value Y' computed according to the relation

$Y' = (g^y \bmod (n))$, wherein "y" is a private non-zero random integer selected by the first member; and

the step of computing a second secret key includes the step computing the second secret key "k1" according to the relation $k1 = (Y'^k \bmod (n))$.

31. The method as recited in Claim 29, wherein the step of sending the first multicast group exchange key to the first member further comprises the first member computing the second secret key "k1" according to the relation $k1 = (K'^y \bmod (n))$.

32. The method as recited in Claim 29, wherein the step of receiving a first user exchange key from a first member comprises the step of providing the first user with the first multicast exchange key only after verifying that the first user is allowed to enter the first multicast group.

33. The method as recited in Claim 29, further comprising the steps of:

determining that a first departing member has left the second multicast group;

selecting a private multicast group non-zero random integer;

generating a second multicast group exchange key based on the private multicast group non-zero random integer, the public non-zero integer "g" and the public prime integer "n";

broadcasting the second multicast group exchange key to each remaining member of the second multicast group;

in response to receiving the second multicast group exchange key, each remaining member computing a third secret key based on the second multicast group exchange key and the second shared secret key; and

establishing a third multicast group whose members include only remaining members of the second multicast group, wherein the third shared secret key provides a second secure channel for communicating between members of the third multicast group over the insecure network.